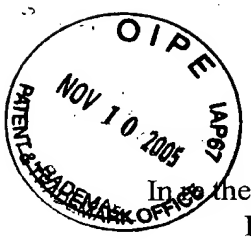
ZFW
AF



PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of:			
Daniell, et al.			
Serial No.:	09/759,932	Art Unit:	2131
Filed:	January 12, 2001	Examiner:	Arani, Taghi T.
For:	SYSTEM AND METHOD FOR PROTECTING A SECURITY PROFILE OF A COMPUTER SYSTEM	Docket No.:	10004557-1

RESPONSE TO NOTIFICATION OF NON-COMPLIANT APPEAL BRIEF

Mailstop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In regard to the outstanding Notice of Non-Compliant Appeal Brief of October 24, 2005, Applicants submit the following remarks.

It is not believed that extensions of time or fees for net addition of claims are required, beyond those which may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. §1.136(a), and any fees required therefor (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Development Company, L.P. Deposit Account No. 08-2025.

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope, with sufficient postage, addressed to: Mailstop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA, 22313-1450 on

11-7-05

Signature: Shanah. East

REMARKS

In the outstanding Notice of Non-Compliant Appeal Brief of October 24, 2005, it is asserted that Applicants' Appeal Brief filed on August 10, 2005, is defective for allegedly failing to contain a concise explanation of the subject matter of each independent claim involved in the appeal. A new summary of the claimed subject matter is set forth below pursuant to M.P.E.P. §1205.03(B). Applicants respectfully assert that the below summary corrects for the alleged defects described by the Notice of Non-Compliant Appeal Brief.

Summary of Claimed Subject Matter

A computer system (e.g., reference numeral 50) of some embodiments comprises memory (e.g., reference numeral 18) and a security application (e.g., reference numeral 52). The security application is configured to display a list of security rules to a user (e.g., page 14, lines 18-19) and to enable ones of the security rules based on user inputs (e.g., page 14, line 23, through page 15, line 2). The security application is configured to lock down resources of the computer system by modifying security settings of the computer system based on which of the security rules are enabled when an activation request is received by the computer system (e.g., page 15, lines 12-18). The security application is configured to store, in the memory, data indicative of the security settings (e.g., page 15, lines 19-22). The security application is configured to perform comparisons between the data and the security settings and to determine when one of the security settings has changed from a first value to another value based on one of the comparisons (e.g., page 16, lines 15-21). The security application is further configured to change the one security setting to the first value in response to the one comparison (e.g., page 16, line 21, through page 17, line 3).

In at least some embodiments, the security application is further configured to transmit a message indicating that the one security setting has changed in response to the one comparison (e.g., page 17, lines 4-15).

A system of some embodiments comprises means for receiving a request for activating a security profile (e.g., reference numeral 50, page 15, lines 3-5 and 12-15). The system also comprises means for modifying security settings of a computer system in response to the request (e.g., reference numeral 50, page 15, lines 5-8), and means for storing data indicative of the modified security settings (e.g., reference numeral 50, page 15, lines 19-22). The system also comprises means for automatically determining when one of the security settings has changed from a first value to another value by periodically comparing the data to the security settings (e.g., reference numeral 50, page 16, lines 15-21), and means for automatically changing the one security setting to the first value in response to a determination by the determining means that the one security setting has changed (e.g., reference numeral 50, page 16, lines 21-25).

In at least some embodiments, the system also comprises means for automatically transmitting, in response to the determination, a message indicating that the one setting has changed (e.g., reference numeral 50, page 17, lines 4-15).

A method of some embodiments comprises receiving a request for activating a security profile (e.g., page 15, lines 3-5 and 12-15). The method also comprises modifying security settings of a computer system in response to the request (e.g., page 15, lines 5-8), and storing data indicative of the security settings, as modified by the modifying (e.g., page 15, lines 19-22). The method further comprises automatically determining when one of the security settings has changed from a first value to another value by periodically comparing the data to the security settings (e.g., page 16, lines 15-21), and automatically changing the one security setting to the

first value in response to a determination in the determining that the one security setting has changed (e.g., page 16, lines 21-25).

In at least some embodiments, the method also comprises automatically transmitting, in response to the determination, a message indicating that the one security setting has changed (e.g., page 17, lines 4-15).

A computer system of some embodiments comprises memory (e.g., reference numeral 18), an operating system (e.g., reference numeral 16), and a security application (e.g., reference numeral 52). The operating system is configured to analyze a machine state to control operation of the computer system. In particular, the machine state includes a security setting associated with a resource of the computer system and indicates whether access to the resource is restricted, and the operating system is configured to analyze the security setting to control access to the resource (e.g., page 10, line 7, through page 11, line 8). The security application is configured to modify the security setting based on a user input and to store, in the memory, data indicative of a state of the security setting, as modified by the security application (e.g., page 15, lines 5-24). The security application is configured to perform a comparison between the data and the security setting to detect an unauthorized change of the security setting (e.g., page 16, lines 15-23). The security application is further configured to automatically change the security setting based on the data in response to a detection of an unauthorized change of the security setting (e.g., page 16, lines 23-25).

In at least some embodiments, the security application is further configured to transmit, in response to the detection, a message indicating that the one security setting has changed (e.g., page 17, lines 4-15).

CONCLUSION

Applicants respectfully request that the Patent Office accept and consider the Appeal Brief filed on August 10, 2005. If the Examiner has any questions or comments regarding this paper, the Examiner is encouraged to telephone Applicants' undersigned counsel.

Respectfully submitted,

THOMAS, KAYDEN, HORSTEMEYER & RISLEY, L.L.P.

By: 

Jon E. Holland
Reg. No. 41,077
(256) 704-3900 Ext. 103

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400